Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-6. (Canceled)

7. (Currently amended): A digital signature verifying method, comprising:

accepting a digital-signature-attached message;

acquiring a log list of a digital signer, wherein said digital-signature-attached message which may have been distributed by said digital signer is to be verified; ~~and~~

checking whether log data of said digital-signature-attached message is registered in said log list[[,]] ;

if the log data is registered in the log list, authenticating that the digital-signature-attached message was distributed by the digital signer; and

checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

8. (Canceled)

9. (Original): The digital signature verifying method of claim 7, wherein said digital-signature-attached message further comprises data from a previously signed message, said method further comprising:

checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included

in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

10. (Original): The digital signature verifying method of claim 9, said method further comprising:

checking whether data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, authenticating that said log list has not been altered.

11. (Original): The digital signature verifying method of claim 7, wherein said log data further comprises a distribution destination, said method further comprising:

acquiring a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list, and

checking whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, authenticating that said log list has not been altered.

12. (Original): The digital signature verifying method of claim 7, wherein said digital-signature-attached message further comprises a timestamp created using a second secret key, said method further comprising:

acquiring a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message; and

checking whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message, and if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, authenticating the validity of the acquired digital signature.

13-20. (Canceled)

21. (Previously presented): A digital signature verifying apparatus, comprising:

a processor interconnected with an input device, wherein:

said input device accepts a digital-signature-attached message to be verified and a log list of a digital signer; and wherein

said processor checks whether log data of said digital-signature-attached message is registered with said log list, and

if the log data is registered with the log list, authenticates that the digital-signature-attached message has been generated by said digital signer,

wherein said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

22. (Canceled)

23. (Original): A digital signature verifying apparatus of claim 21, wherein said digital-signature-attached message further comprises data from a previously signed message, and wherein

said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

24. (Original): A digital signature verifying apparatus of claim 23, wherein said processor checks whether the data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before the log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, said processor authenticates that said log list has not been altered.

25. (Original): The digital signature verifying apparatus of claim 21, wherein said log data further comprises a distribution destination, and wherein:

said processor acquires a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list, and wherein

said processor checks whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, said processor authenticates that said log list has not been altered.

26. (Original): The digital signature verifying apparatus of claim 21, wherein said digital-signature-attached message further comprises a timestamp created using a second secret key, and wherein:

said processor acquires a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message; and wherein

said processor checks whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message, and if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, said processor authenticates the validity of the acquired digital signature.

27-29. (Canceled)

30. (Previously presented): A computer program product for verifying a digital signature, said computer program product comprising:

code that accepts a digital-signature-attached message and a log list from a digital signer; and

code that checks whether log data of said digital-signature-attached message is registered with said log list, and if the log data is registered with the log list, authenticates that the digital-signature-attached message has been generated by said digital signer, wherein said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer; and

a computer readable storage medium for storing the codes.

31-33. (Canceled)

34. (Previously presented): The digital signing method of claim 1 wherein the registering further includes registering the computed data.

35. (Previously presented): The digital signature verifying method of claim 7 wherein the digital-signature-attached message that is registered in the log list includes data based on a previously generated digital signature and on a previous message.

36. (Previously presented): The digital signing apparatus of claim 13 wherein said processor further registers the computed data.

37. (Previously presented): The digital signature verifying apparatus of claim 21 wherein the digital-signature-attached message that is registered in the log list includes data based on a previously generated digital signature and on a previous message.

38. (New): A digital signing system, said system comprising:

a digital signing apparatus;

a timestamp issuing apparatus; and

a digital signature verifying apparatus,

said digital signing apparatus comprising a processor and a communication interface, wherein said processor applies a first secret key to a message or to its hash value to generate a digital signature, said processor transmits said digital signature to said timestamp issuing apparatus by said communication interface and acquires a timestamp in response, and said processor attaches the acquired timestamp to said message to create a digital-signature-attached message,

said timestamp issuing apparatus comprising a processor and a communication interface, wherein said processor generates a timestamp by applying a second secret key to data which includes the digital signature sent by said digital signing apparatus, and a reception time of the digital signature, and said processor transmits said timestamp to said digital signing apparatus,

said digital signature verifying apparatus comprising a processor interconnected with an input device, wherein said input device accepts a digital-signature-attached message to be verified, and said processor acquires a digital signature and time data by applying a public key paired with the secret key of the timestamp apparatus to the timestamp included in said digital-signature-attached message, and thereupon

said processor checks whether date and time indicated by the time data exceeds expiration date and time assigned at said digital signing apparatus, and when the date and time indicated by the time data does not exceed the expiration date and time, said processor authenticates the validity of the said digital signature, and thereupon

said processor authenticates whether said digital signature included in said digital-signature-attached message has been generated for the message included in said digital-signature-attached message, using said digital signature, the message included in said digital-

signature-attached message, and a public key paired with the secret key of the digital signing apparatus.